REMARKS/ARGUMENTS

The Examiner rejected claims 1, 4, 5, 7, 10, 13, 16, and 17 as obvious (35 U.S.C. §103) over Kenner (U.S. Patent No. 6,314,565), Stedman (U.S. Patent No. 6,262,726), and Hsu (U.S. Patent No. 5,894,515). Applicants traverse.

Claims 1, 7, and 13 concern downloading an application program from a remote data processing system for execution by a particular user on a local data processing system, and require: defining and storing a user configuration of the application program corresponding to the particular user of the application program; encrypting and storing the user configuration in a manifest file; initiating a session between the local data processing system and the remote data processing system in response to the particular user requesting the application program; authenticating the particular user in response to the particular user requesting the application program; decrypting the manifest file to produce a decrypted user configuration in response to the user authentication; and responsive to the user authentication, downloading data from the remote data processing system to the local data processing system according to the decrypted user configuration.

The Examiner cited col. 1, lines 13-21 of Hsu as teaching the claim requirement of encrypting and decrypting the manifest file storing the user configuration. (Third Office Action, pgs. 2-3) The cited col. 1 of Hsu discusses encryption and decryption in general and the use of encryption to protect data from an unauthorized user. Nowhere does the cited Hsu anywhere teach or suggest storing the user configuration in a manifest file and then decrypting the manifest file to produce a decrypted user configuration that is used when downloading data from the remote data processing system.

Further, nowhere does the cited Kenner and Stedman teach storing the user configuration in a manifest file that is decrypted in response to user authentication to produce a decrypted user configuration that is used when downloading data from the remote data processing system. The cited col. 7, lines 5-12 and 7-32 of Kenner discusses how a registry file is queried to identify installed codecs and their verison, where applications post and retrieve registry information to determine or alter system and software configuration data. Further, the cited col. 7 mentions that the stored codec information does not need to be in the system registry, and that this information may be updated when the codecs are installed.

Nowhere in the cited col. 7 is there any teaching or suggestion of storing the user configuration in a manifest file and then decrypting the manifest file in response to user authentication to produce a decrypted user configuration that is used when downloading data from the remote data processing system. There is no mention in the cited col. 7 of storing user configuration information or the registry file in a manifest that is decrypted in response to user authentication and used to download data from a remote server.

The cited col. 8, lines 18-29 of Kenner mentions downloading a codec by having an updating system simulate the responses the codec provider would have received upon a user filling out the forms manually, and that the download operation can include exchange of information between the user terminal and the codec provider. The cited col. 9, lines 39-53 discusses an HTTP GET request identifying codec files to download.

Nowhere in the cited cols. 8-9 of Kenner is there any teaching or suggestion of the claim requirement of storing the user configuration in a manifest file and then decrypting the manifest file in response to user authentication to produce a decrypted user configuration that is used when downloading data from the remote data processing system.

The cited col. 6, lines 55-62 of Stedman mentions that to initialize the operating system, the user must enter his or her username and password, and that configuration files keep track of the user, and the desktop layout for the user.

The cited Kenner discusses how a registry file is queried to determine codecs to install and Stedman discusses user authentication. However, nowhere in the cited combination of Kenner and Stedman is there any teaching or suggestion of the claim requirement of storing the user configuration in a manifest file and then decrypting the manifest file in response to user authentication to produce a decrypted user configuration that is used when downloading data from the remote data processing system.

Moreover, even if one were to modify the systems of Kenner and Stedman with Hsu to provide encryption, the proposed modification still does not teach the claim requirements. For instance, modifying the cited Kenner with encryption would provide an encrypted registry file having information used to install a codec. Modifying the cited Stedman with encryption would provide some encrypted authentication. All the combination of references still nowhere teach or suggest the sequence of claim requirements of storing the user configuration in a manifest file,

which is encrypted, and then decrypting the manifest file in response to user authentication to produce a decrypted user configuration that is used when downloading data from the remote data processing system.

The Examiner cited col. 8, lines 18-29 of Kenner as teaching the claim requirement of responsive to the user authentication, downloading data from the remote data processing system to the local data processing system according to the decrypted user configuration. (Third Office Action, pg. 2)

As discussed, the cited col. 8, lines 18-29 mentions downloading a codec by having an updating system simulate the responses the codec provider would have received upon a user filling out the forms manually, and that the download operation can include exchange of information between the user terminal and the codec provider. Nowhere does this cited col. 8 anywhere teach or suggest the claim requirement downloading data from a remote data processing system according to user configuration in a manifest that is encrypted and decrypted in response to user authentication.

Accordingly, claims 1, 7, and 13 are patentable over the cited combination because the cited combination does not teach or suggest all the claim requirements.

Claims 4, 5, 10, 16, and 17 are patentable over the cited art because they depend from claims 1, 7, and 13, which are patentable over the cited art for the reasons discussed above. Certain of these claims provide additional grounds of patentabiliyt over the cited art.

Claims 4, 10, and 16 depend from claims 1, 7, and 13 and further require building the application program pursuant to the user configuration decrypted from the manifest file responsive to a second authentication. Thus, the combination of these claims with the base claims require that the user configuration in the manifest is used to both download data from the remote data processing system and then build the application program. Applicants submit that nowhere does the cited art teach or suggest that user configuration in manifest be used to both download data from the remote data processing system and then build the application program.

The Examiner cited col. 8, lines 30-41 of Kenner as teaching the additional requirements of claims 4, 10, and 16. (Third Office Action, pg. 3) Applicants traverse.

The cited col. 8 discusses how a codec is installed according to instructions set forth in the script file and that the codec's own installation program will take over once started.

Although the cited col. 8 mentions how a script file is used to install a program, the cited script file does not comprise a user configuration of the application. Nowhere does the cited col. 8 anywhere disclose that the script file is a user configuration. Further, the Examiner previously cited the registry file of Kenner as the user configuration information. Nowhere does the cited Kenner anywhere teach or suggest that the user registry file, which the Examiner likened to the user configuration information, be used to build the application program. Instead, in the cited Kenner, the script file is used to configure the application, which is not the same component used to download the data as claimed.

Moreover, nowhere does the cited art anywhere disclose that the application is built in response to a second authentication as claimed.

Accordingly, claims 4, 10, and 16 provide additional grounds of patentability over the cited art.

The Examiner rejected claims 5, 11, and 17 as obvious for the reasons discussed in the second office action dated Oct. 28, 2003, paper no. 7 ("Second Office Action"). (Third Office Action, pg. 3) On page 4 of the Second Office Action, the Examiner cited col. 8, lines 30-41 of Kenner as teaching building the application program according to a configuration and that the encryption/decryption of Hsu teaches encrypting the manifest. (Second Office Action, pg. 4) Applicants traverse.

As discussed the cited col. 8 discusses the use of a script file to install a program, which is different than cited registry file the Examiner likened to the user configuration. Thus, for the reasons discussed with respect to claims 4, 10, and 16, the cited script file does not comprise user configuration as claimed.

Accordingly, claims 5, 11, and 17 provide additional grounds of patentability over the cited art.

The Examiner referenced the prior art obviousness rejection of claims 3, 6, 9, 12, 15, and 18 in the previous Second Office Action, in which the Examiner rejected these claims as obvious (35 U.S.C. §103) over Kenner, Stedman, Hsu and Hayes (U.S. Patent No. 6,205,476). Applicants traverse.

First off, these claims 3, 6, 9, 12, 15 are patentable over the cited art because they depend from claims 1, 7, and 13, which are patentable over the cited art for the reasons discussed above. Moreover, certain of these claims provide additional grounds of patentability over the cited art.

Claims 3, 9, and 15 depend from claims 1, 7, and 13 and further require that the manifest file is stored on the remote data processing system and downloading the manifest file from the remote data processing system to the local data processing system. The downloaded manifest file is decrypted to produce a downloaded user configuration in response to the user authentication, and wherein the data is downloaded from the remote data processing system according to the downloaded user configuration.

The Examiner referenced the art cited on page 6 of the Second Office Action (Third Office Action, pg. 4) as teaching the requirements of these claims. In the Second Office Action, the Examiner cited col. 22, lines 55-59 of Hayes as teaching storing user specific application configuration preferences and transmitting them to the local user system. (Second Office Action, pg. 5).

The cited col. 22 of Hayes mentions storing the configuration preferences for the end user on the server and downloading a set of preferences stored for a given context to a workstation when requested by a user.

Although the cited Hayes mentions storing configuration preferences on a server and downloading to a workstation, nowhere does the cited Hayes anywhere teach the claim requirement of downloading a manifest file that is decrypted and that data is downloaded from the remote data processing system according to the downloaded user configuration. Nowhere does the cited Hayes anywhere teach or suggest downloading user configurations in a manifest to use to subsequently download data from a remote data processing system.

Accordingly, claims 3, 9, and 15 provide additional grounds of patentability over the cited art.

Claims 6, 12, and 18 depend from claims 1, 7, and 13 and further require that the user configuration comprises data describing the particular user, the particular user's application program configuration, and resources for which the particular user is authorized.

The Examiner referenced the art cited on page 6 of the Second Office Action (Third Office Action, pg. 4). In the Second Office Action, the Examiner cited col. 1, lines 58-63 as teaching the additional requirements of these claims.

The cited col. 1 mentions that user profiles may be stored on the server. However, the cited col. 1 nowhere discloses that the cited user profiles are placed in a manifest and used to download data from a remote processing system to the local processing system as claimed.

Accordingly, claims 6, 12, and 18 provide additional grounds of patentability over the cited art.

Conclusion

For all the above reasons, Applicant submits that the pending claims 1, 3-7, 9-13, and 15-18 are patentable over the art of record. Applicants have not added any claims. Nonetheless, should any additional fees be required, please charge Deposit Account No. 09-0460.

The attorney of record invites the Examiner to contact him at (310) 553-7977 if the Examiner believes such contact would advance the prosecution of the case.

Dated: July 16, 2004

By:

David W. Victor
Registration No. 39,867

Please direct all correspondences to:

David Victor
Konrad Raynes & Victor, LLP
315 South Beverly Drive, Ste. 210
Beverly Hills, CA 90212
Tel: 310-553-7977
Fax: 310-556-7984